IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Issue-7, July 2019 E-ISSN: 2347-2693

A Review on Analysis of TPA model for Secure Information Retrieval in Cloud Computing

Nitin Kumar Sahu[1*], Anuj Kumar Pal[2]

[1]Department of CSE, Research Scholar BIRT, RGPV, Bhopal, India
[2]Department of Science and Technology, BIRT, Bhopal, India

[*]*Corresponding Author: sahu.nitin2803@gmail.com, Tel.: +91-839077614*

DOI: https://doi.org/10.26438/ijcse/v7i7.161164 | Available online at: www.ijcseonline.org

Accepted: 12/Jul/2019, Published: 31/Jul/2019

***Abstract*—** Today's businesses are interested in secure data and their applications can be accessible from anywhere using any device. It is able to achieve using cloud technology, but there are implicit challenges to making it realism. What can enterprise businesses do to reap the benefits of cloud technology while ensuring a secure environment for sensitive information? Recognizing those challenges is the first process to finding solutions that work. Increasingly many companies plan to move their local data management systems to the cloud and store and manage their product details on cloud servers. An accompanying issue is how to protect the security of the commercially confidential data, while preserve the ability to search the data. In this paper we are analysis of different securities scheme for encryption of item information and also for data search scheme in cloud computing.

***Keywords*—**Cloud Computing, Cloud Security, Security issues, Information Security.

I. INTRODUCTION

Very large amounts of user data are outsourced to cloud servers, the data owner need to encrypt the abovementioned sensitive data, plain text based data search are no longer suitable. In addition, bonded by network bandwidth and local storage device capacity constraints, users find it not possible to re-download all the data to a local device and later decrypt them for use. Based on the above concern, privacy-preserving data search method were born, designed to make sure that only genuin users based on identifiers or keywords, have the accessibility to search the data. These schemes secure users private data but enable the server to return the cipher text file according to the query request. Thus, we can make sure the security of user data and privacy while not inordinately reducing the query efficiency.

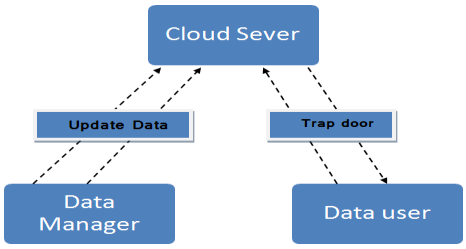

Figure 1: Encrypted information retrieval system model

Cloud computing is taken into account one in all the foremost dominant paradigms within the data Technology (IT) business of late. It offers new price effective services on-demand like package as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). However, with all of those services promising facilities and edges, there ar still variety of challenges related to utilizing cloud computing like knowledge security, abuse of cloud services, malicious corporate executive and cyber-attacks. Among all security needs of cloud computing, access management is one in all the elemental needs so as to avoid unauthorized access to systems and defend organizations assets. Although, varied access management models and policies are developed like obligatory Access management (MAC) and Role based mostly Access management (RBAC) for various environments, these models might not fulfill cloud's access management needs. this is often as a result of cloud computing contains a numerous set of users with totally different sets of security needs. It conjointly has distinctive security challenges like multi-tenant hosting and heterogeneousness of security policies, rules and domains. This paper presents a close access management demand analysis for cloud computing and identifies vital gaps, that aren't consummated by standard access management models. This paper conjointly proposes associate degree access management model to fulfill the known cloud access management needs. we tend to believe that the planned

model can't solely make sure the secure sharing of resources among potential untrusted tenants, however conjointly has the capability to support totally different access permission to constant cloud user and offers him/her the power to use multiple services firmly.

II. RELATED WORK

Ying-si zhao et al. [1] "Secure and Efficient Product Information Retrieval in Cloud Computing" In this paradigm Cloud computing could be a promising service which will organize immense quantity of knowledge technology resources in associate economical and versatile manner. Increasingly varied firms attempt to move their native knowledge management systems to the cloud and store and manage their product data on cloud servers. Associate in one more challenge is a way to shield the protection of the commercially confidential knowledge, while maintaining the ability to search the users data. In this paper, a privacy-preserving knowledge search theme is projected, which will support each the identifier-based and feature-based product searches. Specifically, 2 novel index trees area unit made and encrypted, which will be searched while not knowing the plain text knowledge. Analysis and simulation results demonstrate the protection and potency of our theme.

ZHEN WANG et al. [2] " Enhanced Instant Message Security and Privacy Protection Scheme for Mobile Social Network Systems" The projected theme supports denial of replaying attack and denial of forgery attack by utilizing timestamps and therefore the elliptic curve digital signature formula. It supports multiple varieties of messages (such as document and transmission messages) and prevents privacy outpouring by storing sent and received messages with cipher text. we have a tendency to established the protection of the projected theme underneath the elliptic curve distinct log assumption and therefore the CDH assumption. The comparison results of the projected theme with different themes and therefore the results of Associate in Nursing experiment show that it's a comprehensive secure scheme with high security and sensible usefulness.

Cao et al. [3] First proposed a basic privacy-preserving multi-keyword ranked search scheme based on a secure kNN algorithm. A set of strict privacy requirements are established, and two schemes are later proposed to improve the security and search experience. However, an apparent drawback of this scheme is that the search efficiency is linear with the cardinality of the document collection, and consequently, it cannot be used to process extremely large document databases.

Xia et al. [4] designed a keyword balanced binary tree to arrange the document vectors and planned a ''Greedy Depth-First Search'' algorithmic program to boost the search potency. Moreover, the index tree is updated dynamically with an appropriate communication burden.

Yusof et al. [5] This paper presents a close access management demand analysis for cloud computing and identifies vital gaps, that aren't consummated by conventional access management models. This paper conjointly proposes associate degree access management model to meet the known cloud access management needs. we have a tendency to believe that the projected model can not solely make sure the secure sharing of resources among potential untrusted tenants, but conjointly has the capability to support completely different access permission to an equivalent cloud user and gives him/her the flexibility to use multiple services firmly.

Akhilesh Yadav et al.[6] "Securing Cloud Computing Environment using Quantum Key Distribution" Nowadays, data Technology cluster is undergone vital shift in computing and protective business worth by exploitation well-built, executable and authentic replacement of Cloud Computing. Cloud Computing could be a up to date process design that has another style of model. This paper proposes as a service of Advanced Quantum Cryptography in Cloud Computing. This paper discusses the safety problems with cloud computing and therefore the role of cryptography technique in Cloud computing to counterpoint the data Security.

Rongzhi Wang "Research on Data Security Technology Based on Cloud Storage"[7] Encryption storage, integrity verification, access management and verification so on. Through the info segmentation and refinement rules algorithmic rule to optimize the access management strategy, mistreatment information|the info|the information} label verification cloud data integrity, mistreatment duplicate strategy to confirm the info convenience, the peak of authentication to strengthen security, attribute encoding methodology mistreatment signcryption technology to enhance the algorithmic rule potency, the employment of your time encoding and DHT network to confirm that the cipher text and key to delete the info, therefore on establish a security theme for cloud storage has the characteristics of privacy protection.

III. CLOUD SECURITY CHALLENGES

DDoS attacks

As additional and additional businesses and operations move to the cloud, cloud suppliers have become an even bigger target for malicious attacks. Distributed denial of service (DDoS) attacks is additional common than ever before.

Verisign rumored IT services, cloud and SaaS was the foremost often targeted trade throughout the primary quarter of 2015.

A DDoS attack is meant to overwhelm web site servers therefore it will now not reply to legitimate user requests. If a DDoS attack is triple-crown, it renders a web site useless for hours, or perhaps days. this may lead to a loss of revenue, client trust and complete authority.

Complementing cloud services with DDoS protection isn't any longer simply sensible plan for the enterprise; it's a necessity. Websites and web-based applications area unit core elements of twenty first century business and need progressive security.

Data breaches

Known information breaches within the U.S. hit a record-high of 738 in 2014, in line with the fraud centre, and hacking was (by far) the amount one cause. That's an out of this world data point and solely emphasizes the growing challenge to secure sensitive information.

Traditionally, IT professionals have had nice management over the network infrastructure and physical hardware (firewalls, etc.) securing proprietary information. within the cloud (in personal, public and hybrid scenarios), a number of those controls square measure relinquished to a trusty partner. selecting the proper marketer, with a robust record of security, is significant to overcoming this challenge.

Data loss

When business vital data is affected into the cloud, it's apprehensible to be anxious with its security. Losing information from the cloud, either tho' accidental deletion, malicious change of state (i.e. DDoS) or associate act of nature brings down a cloud service supplier, can be fatal for associate enterprise business. typically a DDoS attack is merely a diversion for a larger threat, like an effort to steal or delete information.

To face this challenge, it's imperative to make ensure there's a disaster recovery method in situ, in addition as associate integrated system to mitigate malicious attacks. additionally, protective each network layer, as well as the applying layer (layer 7), ought to be integral to a cloud security answer.

Points

One of the nice advantages of the cloud is it may be accessed from anyplace and from any device. But, what if the interfaces and arthropod genus users move with aren't secure? Hackers will realize these varieties of vulnerabilities and exploit them.

A activity net application firewall examines protocol requests to a web site to confirm it's legitimate traffic. This always-on device helps defend net applications from security breaches.

Notifications and alerts

Awareness and correct communication of security threats could be a cornerstone of network security and therefore the same goes for cloud security. Alerting the suitable web site or application managers as shortly as a threat is known ought to be a part of a radical security set up. Speedy mitigation of a threat depends on clear and prompt communication therefore steps may be taken by the correct entities and impact of the threat reduced.

IV. PROPOSED WORK

• A product information outsourcing and searching system model including the data owner, cloud server and data users is designed.
• Two index structures supporting efficient product retrieval are constructed. Moreover, corresponding search algorithms are also proposed
• cloud storage auditing protocol with secure outsourcing of key updates is composed by seven algorithms (SSetup, EUpdate, VESK, DESK, AuthGen, Proof- Gen, ProofVerify and Check Proxy TPA), shown below:
• SSetup: the system setup algorithm is run by the client. It takes as input a security parameter k and the total number of time periods T, and generates an encrypted initial client's secret key ESK0, a decryption key DK and a public key PK. Finally, the client holds DK, and sends ESK0 to the TPA.
• EUpdate: the encrypted key update algorithm is run by the TPA. It takes as input an encrypted client's secret key ESKj , the current period j and the public key PK, and generates a new encrypted secret key ESKj+1 for period j + 1.
• VESK: the encrypted key verifying algorithm is run by the client. It takes as input an encrypted client's secret key ESKj , the current period j and the public key PK, if ESKj is a well-formed encrypted client's secret key, returns 1; otherwise, returns 0.
• DESK: the secret key decryption algorithm is run by the client. It takes as input an encrypted client's secret key ESKj , a decryption key DK, the current period j and the public key PK, returns the real client's secret key SKj in this time period.
• AuthGen: the authenticator generation algorithm is run by the client. It takes as input a file F, a client's secret key SKj , the current period j and the public key PK, and generates the set of authenticators _ for F in time period j.
• ProofGen: the proof generation algorithm is run by the cloud. It takes as input a file F, a set of authenticators a challenge a time period j and the public key PK, and generates a proof P which proves the cloud stores F correctly.

• Checking algorithm for proxy server of TPA Proof Verify: the proof verifying algorithm is run by the TPA. It takes as input a proof P, a challenge a time period j, and the public key PK, and returns
• A series of simulations are conducted to illustrate the security and efficiency of the proposed scheme.

V. CONCLUSION

In this paper, we designed a secure and efficient product information retrieval scheme based on cloud computing. Specifically, two index structures, including a hash value AVL tree and a product vector retrieval tree, are constructed, and they support an identifier-based product search and feature-vector-based product search, respectively. By checking a proxy server we will find out the fault in encryption. Cloud must be safe from all the external threats, so there will be a strong and mutual understanding between the client end and the cloud server end. Main goal of cloud computing is securely store and transmit the data in cloud.

REFERENCES

[1] YING-SI ZHAO "*Secure and Efficient Product Information Retrieval in Cloud Computing*" Received February 10, 2018, accepted March 11, 2018, date of publication March 19, 2018, date of current version April 4, 2018
[2] M. J. Atallah, K. Pantazopoulos, J. R. Rice, and E. ESpafford, "*Secure outsourcing of scientific computations*," Trends in Software Engineering, vol. 54, pp. 215-272
[3] Cao et al. "*Privacy-preserving multi-keyword ranked search over encrypted cloud data*". ieee infocom 2011
[4] Jin Li, Gansen Zhao, Xiaofeng Chen, Dongqing Xie, "*Fine-grained Data Access Control Systems with User Accountability in Cloud Computing*", IEEE International Conference on Cloud Computing Technology and Science, 2010.
[5] Younis A. Younis, Kashif Kifayat, Madjid Merabti, "*An access control model for cloud computing*", Elsevier journal of information security and applications, 2014.
[6] Rongzhi Wang "*Research on Data Security Technology Based on Cloud Storage*".
[7] Akhilesh Yadav et al. *"Securing Cloud Computing Environment using Quantum Key Distribution"*
[8] C. Wang, Q. Wang, K. Ren, N. Cao, W. Lou *"Toward secure and dependable storage services in cloud computing"* IEEE Trans. Services Comput., 5 (2) (2012), pp. 220-232
[9] Duncan, Adrian, Sadie Creese, and Michael Goldsmith . "*Insider attacks in cloud computing."* Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. IEEE,2012..

Authors Profile

Mr. Nitin Kumar Sahu pursuing Master of Technologh from BIRT, Bhopal.

Mr Anuj Kumar Pal .He is currently working as Assistant Professor in Department of Computer Science and Technology in BIRT Bhopal, India.

